(ICETETSM-17)
ISBN: 978-93-86171-45-0

PROTECTING WEB SERVERS FROM DISTRIBUTED DENIAL OF SERVICE ATTACKS

[1]Prof.A.N.Banubakode, [2]Badal Mehta,
[3]Tanmay Modak, [4]Vrushal Chaudhary
[1,2,3,4,5] JSPM's RSCOE, S.P. Pune University, Pune, (India)

ABSTRACT

Recently many prominent websites faced the Distributed Denial of Service (DDOS) attacks. While former security threats could be faced by tight security policy and measures like using firewalls, vendor patches etc. These DDOS are new in such a way that there is no completely satisfying protection as yet. There are certain solutions based on class based routing mechanisms in the LINUX kernel which prevent most severe impacts of DDOS. However, these do not provide complete security to the web server and hence there is a need to focus on other defense mechanisms.

We propose to introduce a concept called Honeypot in which we create a proxy server so as to lure attackers. In this system we can identify the attacker and can be notified immediately.

Index Terms: Honeypot, Security, Attack Detection.

I. INTRODUCTION

The extremely widely used World Wide Web environment provides a rich set of targets for motivated attackers. The disruption of service is the main goal of the attack. To prevent these attacks and prevent these servers from DDOS attacks we are implementing a system which is going to use 'Honeypot' system and 'AES 128-bit Algorithm'

Here, we use a Banking application where online transactions can be performed and attacks like SQL injection , Brute Force Attacks , URL injection, Cross site scripting attack can be detected, Personal information of the user get stored in database in encrypted format, dynamic password and PIN is generated and sent to the user on his email. After every transaction user gets notification by message. User can see his account details and mini statements. The internet was originally designed to facilitate the research and educational communities with an open and scalable network. Due to the increased number of cyber-attacks over the past years, solving the security issues has gained more importance. DOS and DDOS attacks being the most popular ones. After detailed study of DOS and DDOS attacks on the internet their victims and possible form of attacks, we realize that there are a lot of challenges in defending against these attacks. Since most of the DDOS attacks are due to the

ISBN: 978-93-86171-45-0

vulnerability in the Protocols at different layers of TCP/IP model of the internet, our study is mainly focused on exploration of different types of DDOS attacks and their effects on the server.

II. LITERATURE SURVEY

System uses some techniques are as follow :

Honeypot System :

A honeypotis a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems.

Honeypots are classified as following on the basis of design criteria:

1. **Pure honeypots** : Are full-fledged production systems. The activities of the attacker are monitored by using a casual tap that has been installed on the honeypots link to the network.
2. **High-interaction honeypots** : Imitate the activities of the production systems that host a variety of services and, therefore, an attacker may be allowed a lot of services to waste his time.
3. **Low-interaction honeypots** : Simulate only the services frequently requested by attackers.

AES 128 bit Encryption Decryption algorithm :

The features of AES are as follows :

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java.

III. MATHEMATICAL MODEL

S= {S, s, X, Y, T, f_{main}, DD, NDD, f_{friend}, memory shared, CPU_{count}}

- **S (system)**:- Is our proposed system which includes following tuple.
- **s (initial state at time T)** :-GUI of Protecting Web Server From DDOS Attack.. The GUI provides space to enter a query/input for user.
- **X (input to system)** :- Input Query. The user has to first enter the query. The query may be ambiguous or not. The query also represents what user wants to search.
- **Y (output of system)**:- List of URLs with Snippets. User has to enter a query into Protecting Web Server From DDOS Attack. then Protecting Web Server From DDOS Attack. generates a result which contains relevant and irrelevant URL's and their snippets.
- **T (No. of steps to be performed)**:- **6**. These are the total number of steps required to process a query and generates results.

ISBN: 978-93-86171-45-0

- **f_{main}(main algorithm)** :- It contains Process P. Process P contains Input ,Output and subordinates functions. It shows how the query will be processed into different modules and how the results are generated.
- **DD (deterministic data)**:- It contains Database data. Here we have considered Ebanking database i.e. database related to banking system which contains number of ambiguous queries. Such queries are user for showing results. Hence, Ebanking database is our DD.
- **NDD (non-deterministic data)**:- No. of input queries. In our system, user can enter numbers of queries so that we cannot judge how many queries user enters into single session. Hence, Number of Input queries are our NDD.
- **f_{friend}** :- WC And IE. In our system, WC and IE are the friend functions of the main functions. Since we will be using both the functions, both are included in f_{friend} function. WC is Web Crawler which is bot and IE is Information Extraction which is used for extracting information on browser.
- **Memory shared**: - Database. Database will store information like list of receivers, registration details and numbers of receivers. Since it is the only memory shared in our system, we have included it in the memory shared.
- **CPU_{count}**: - 2. In our system, we require 1 CPU for server and minimum 1 CPU for client. Hence, CPU_{count} is 2.

Subordinate functions:

❑ Identify the processes as P.

S= {I, O, P....}

P= {WP, WD}

Where,

- ➢ WP is Web Portal for Banking
- ➢ WD is Honeypot System to defence Web Portal.
- ➢ P is processes.

❑ **WC= {U, MAX, CP}**

Where,

- ➢ U=input Query
- ➢ MAX = {1, 2, 3, … , n}
- ➢ CP is output of WD which prevents our system from different attacks

❑ **IE= {CP, NLP Techniques, Info}**

Where,

- ➢ CP is incoming attacks

ISBN: 978-93-86171-45-0

- NLP is preventing attacks by filtering,script cross checking,query optimization

IV. TECHNOLOGIES TO BE USED

Our system uses the following technologies:

- **Java**

Java is designed for applications that are portable and also have high-performance for the widest range of computing platforms .By making applications available across heterogeneous environments, businesses can provide more and more services and boost end-user productivity, communication, and collaboration—and dramatically reduce the cost of ownership of both enterprise and consumer applications.

The previous and reference implementation of Java compilers, virtual machines, and class libraries were released by Sun under proprietary licenses. As per the Java Community Process specifications, by May 2007,Sun has relicensed many of its Java technologies under the General Public License. Others have also developed some alternative implementations of these Sun technologies, such as the GNU Compiler for Java (byte code compiler), GNU Classpath (standard libraries), and IcedTea-Web (browser plugin for applets).

- **Honeypot System**

It is a computer security mechanism which helps in detecting, deflecting, or, in some manner, counteract attempts made forunauthorized use of information systems.

Based on design criteria, honeypots can be classified as:

1. Pure Honeypots: Are full-fledged production systems.A casual tap is installed on the network link of the Honeypot so as to monitor attacker's activity.
2. High-interaction honeypots: Imitate the activities of the production systems that host a variety of services and, therefore, an attacker may be allowed a lot of services to waste his time.
3. Low-interaction honeypots: Simulate only the services frequently requested by attackers.

- **AES 128 bit Encryption Decryption algorithm**

The Advanced Encryption Standard or AES is a symmetric block cipher developed by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data.

The features of AES are as follows :

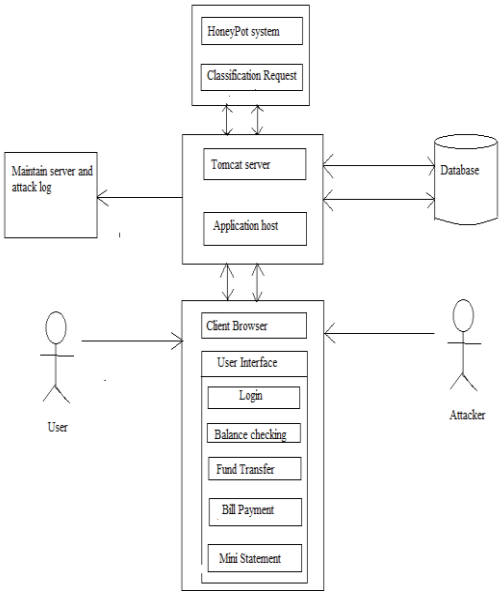
• Symmetric key-Symmetric block cipher
• 128-bit data, 128/192/256-bit keys
• Stronger and faster than Triple-DES

(ICETETSM-17)
ISBN: 978-93-86171-45-0

• Provide full specification and design details

• Software implementable in C and Jav

V. PROPOSED SYSTEM



This is a Banking wed application which provides various functionalities to User and Admin. Admin can approve or reject user application. Admin can search customer by account number or customer name. Admin can see logs of attacks . User can do online transaction like Fund Transfer , Bill Payments (electricity bill, ,income tax, mobile recharge). The application is prevented by detecting different attacks such as SQL injection , URL injection , Cross site Scripting attack and Brute force attack. User will get randomly generated username , password and pin number on his email. After every transaction user will get notification by message . User can see his account details and mini statement . AES-128 bit encryption and decryption is used for storing user details .In this application HoneyPot System is implemented for detecting hackers which attacks on the system externally by using communication protocols

5.1 PRODUCT PERSPECTIVE

Main Perspective of the proposed system is to detect Hackers' attacks and provide the system with security.

This is really helpful in Transaction based systems like Banking, Online Shopping, also in applications where we are storing our personal data.

We are implementing this system to avoid problems which may cause entire region of Internet connectivity to be at stake without the attacker's knowledge or intent by some flimsy network infrastructure equipment or an incorrectly configured network, in case the attack is conducted on a large scale.

ISBN: 978-93-86171-45-0

5.2 PRODUCT FUNCTION

There are types of user who can access this system:

1. Customer

System is applied on Banking Application.Here User can do online transactions-

1. Bill Payments (electricity bill, income tax, mobile recharge).

2. Fund transfer.

Checking of Detection and prevention of multiple attacks like-

1. SQL injection.

2. Brute force attack.

3. URL injection.

4. Cross site Scripting attack.

Personal information of customer gets stored into the database in the encrypted format.

Dynamic password, PIN generation and sending it to user on his mail.

After every transaction User will get notification by message.

User can see his account details and Mini statement.

2. Admin

Able to Approve or reject application.

To Search customer by account number or customer name.

Able to check the logs of attacks.

Different types of hackers are detected using honeypot system.

5.3 USER CHARACTERISTICS

1. System provides Admin and User Log-in form.

2. Provides User Registration form, using this user can register in to the system.

3. System provides Fund Transfer form.

4. Bill Payments form provided to users.

5. User is able to get Mini statement using messages.

6. It gives Hacker detection form which is able to show hackers' details.

VI ALGORITHM

Step 1: User Registration

Step 2: Admin Login

Step 2.1:Approve/Reject User Application

Step 2.2: Search Customer

Step 2.3 :View Customer List

Step 3: User Login

Step 3.1 : View Account Details

ISBN: 978-93-86171-45-0

Step 3.2 : Check Mini Statement

Step 3.3 : Fund Transfer

Step 3.4 : Bill Payments

Step 3.5 : Update Profile

Step 3.6 : Change Password

Step 4: Intruder Attacks on System

Step 4.1: Attack Detection

-SQL injection

-URL injection

-Brute Force Attack

-Cross Site Scripting Attack

Step 4.2: Attack Prevention through Honeypot.

Step 4.3: Maintain Attack Logs

Step 5: Stop

VII CONCLUSION

In this paper, we present a brief survey of the origin of DDoS attacks, and some methods which are developed for the detection and prevention of these DDOS attacks. The necessary factor in inhibiting a DoS attack is to enhance the reliability of global network infrastructure. We observed that most of the approaches deal with attack traffic detection and filtering near the target. DDoS attack is one of the major threats to both network service providers and legitimate customers. New vulnerabilities to intrude systems are being continuously explored by the attackers. We noticed that most of the protocols are vulnerable and prone to DoS attacks. Therefore, we need to devise an effective and integrated solution in prevention of DDoS attacks by upgrading the hardware together with patching software vulnerabilities. We conclude that in spite of significant development in the area of detection, identification and prevention of DDoS attacks, yet the area is worth researching.

VIII FUTURE RESESARCH DIRECTION

Using such technology, we can detect Hackers.System provides Honeypot system using this we can analyze. Hackers. When this is on we will able to get Hackers' information. Proposed System checks attacks related with Bank transaction, which is very helpful.

REFERENCES

1. 1,2Khan Zeb, 2Owais Baig, 2Muhammad Kamran Asif "DDoS Attacks and Countermeasures in Cyberspace"

2. Nhu-Ngoc Dao1, Junho Park1, Minho Park2, and Sungrae Cho1 "A Feasible Method to combat against DDoS Attack in SDN Network"

3. Manjiri Jog, MaitreyaNatu , Sushama Shelke "Distributed Capabilities-based DDoS Defense"

ISBN: 978-93-86171-45-0

4. FouadGuenane∗, Michele Nogueira†, Ahmed Serhrouchni∗ "DDOS Mitigation Cloud-Based Service"

5. S. C. . X. Wang, "Signing Me onto Your Accounts throughFacebook and Google: A Traffic-Guided Security Study ofCommercially Deployed Single-Sign-On Web Services," in *Security and Privacy (SP), 2012 IEEE Symposium*, 2012.

6. "2013 State of Social Media Spam," Nexgate, Tech. Rep., 2013. [Online]. Available: http://nexgate.com/wp-content/uploads/2013/09/ Nexgate-2013-State-of-Social-Media-Spam-Research-Report. Pdf

7. S. Sezer, S. Scott-Hayward, P. Chouhan, B. Fraser, D. Lake, J. Finnegan, N. Viljoen, M. Miller, and N. Rao, "Are we ready for SDN? Implementationchallenges for software-defined networks," *IEEE Communications Magazine*, vol. 51, no. 7, 2013.

8. S. Shin and G. Gu, "Attacking Software-defined networks: a first feasibility study," in *Proc. the second ACM SIGCOMM workshop on Hottopics in software defined networking*, 2013.